PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-231760
(43)Date of publication of application : 22.08.2000

(51)Int.Cl. G11B 20/10
G09C 1/00
G11B 19/04
H04L 9/08

(21)Application number : 11-344396
(22)Date of filing : 03.12.1999
(71)Applicant : SONY CORP
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO

(30)Priority
Priority number : 10352975 Priority date : 11.12.1998 Priority country : JP

(54) DEVICE AND METHOD TO RECORD INFORMATIONDEVICE AND METHOD TO REPRODUCE INFORMATION AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To decode ciphered data using an old generation secret key even though the secret key is updated.
SOLUTION: In an optical disk 7the generation of a sector key Eksin which ciphered contents are writtenis written. A generation discriminating circuit 49 discriminates the generation of the key Eks used in the ciphering. A Km memory 44 outputs a master key Km corresponding to the discriminated generation to an Ekd decoding circuit 46. The circuit 46 decodes a ciphered disk key Ekd by using the key Km. And Ekd decoding circuit 47 decodes the ciphered sector key Eks by using a disk key Kd to obtain a sector key Ks. A contents data decoding circuit 48 decodes ciphered contents data by employing the key Ks.

CLAIMS

[Claim(s)]
[Claim 1]The Information Storage Division device which records data on a removable recording mediumcomprising:
A memory measure which memorizes at least one or more generations' secret key.
A creating means which generates the 1st key from medium identification information and said secret key of said recording medium.
The 1st encoding means that enciphers the 2nd key used in order to encipher said data recorded on said recording medium with said 1st key.
The 1st recording device that records said 2nd key enciphered by said 1st encoding means on said recording medium with a generation number of said 1st key.

[Claim 2]Have further the 1st random number generation means that generates said medium identification information as a random numberand said 1st encoding meansThe Information Storage Division device according to claim 1 characterized by making said 1st random number generation means generate a random number used as said 2nd key when said 2nd key is read from said recording medium when said recording medium has said 2nd key beforehandand said recording medium does not have said 2nd key.
[Claim 3]The 2nd random number generation means that generates a random number used as the 3rd key that enciphers said data which said recording medium is divided per two or more recordsand is recorded on said record unit for said every record unitThe 2nd encoding means that enciphers said 3rd key generated by said 2nd random number generation means with said 2nd keyThe Information Storage Division device according to claim 2 having further the 2nd recording device that records said 3rd key enciphered by said 2nd encoding means per record of said recording medium.
[Claim 4]The Information Storage Division device according to claim 2 whenever said 2nd key changes a generation of said secret key while being made into a peculiar value for said every recording mediumwherein it is newly generated by said 1st random number generation means.
[Claim 5]The Information Storage Division device according to claim 1wherein said memory measure memorizes said secret key of one generation and generates said secret key of other generations by an operation.
[Claim 6]The Information Storage Division device according to claim 1wherein a generation number of said 1st key corresponds to a generation of said secret key used by said creating means.
[Claim 7]An Information Storage Division method of the Information Storage Division device which records data on a removable recording medium characterized by comprising the following.
A storage control step which controls memory to memorize at least one or more

generations' secret key.
A generation step which generates the 1st key from medium identification information and said secret key of said recording medium.
The 1st encryption step that enciphers the 2nd key used in order to encipher data recorded on said recording medium with said 1st key.
The 1st record control step that controls record to record said 2nd key enciphered by processing of said 1st encryption step on said recording medium with a generation number of said 1st key.

[Claim 8]Said medium identification informationincluding further the 1st random number generation step that makes it generate as a random number in processing of said 1st encryption step. When said recording medium has said 2nd key beforehandsaid 2nd key is read from said recording mediumAn Information Storage Division method according to claim 7 generating a random number which serves as said 2nd key by processing of said 1st random number generation step when said recording medium does not have said 2nd key.
[Claim 9]Said recording medium is divided per two or more records.
The 2nd random number generation step that generates a random number used as the 3rd key that enciphers said data recorded on said record unit for said every record unitThe 2nd encryption step that enciphers said 3rd key generated by processing of said 2nd random number generation step with said 2nd keyAn Information Storage Division method according to claim 8 by which the 2nd record control step that controls record to record said 3rd key enciphered by processing of said 2nd encryption step per record of said recording medium being included further.

[Claim 10]An Information Storage Division method according to claim 8 whenever said 2nd key changes a generation of said secret key while being made into a peculiar value for said every recording mediumwherein it is newly generated by processing of said 1st random number generation step.
[Claim 11]An Information Storage Division method according to claim 7 controlling memory by processing of said storage control step to memorize said secret key of one generationand generating said secret key of other generations by an operation.
[Claim 12]An Information Storage Division method according to claim 7wherein a generation number of said 1st key corresponds to a generation of said secret key used by processing of said generation step.
[Claim 13]A program characterized by comprising the following for Information Storage Division devices which records data on a removable recording medium.
A storage control step which controls memory to memorize at least one or more generations' secret key.

A generation step which generates the 1st key from medium identification information and said secret key of said recording medium.
An encryption step which enciphers the 2nd key used in order to encipher data recorded on said recording medium with said 1st key.
A record control step which controls record to record said 2nd key enciphered by processing of said encryption step on said recording medium with a generation number of said 1st key.

[Claim 14]An information reproducing device which reproduces data currently recorded on a removable recording mediumcomprising:
A memory measure which memorizes at least one or more generations' secret key.
The 1st reading means that reads a generation number of the 2nd key enciphered with the 1st keyand said 1st key that enciphered said 2nd keyand medium identification information of said recording medium from said recording medium.
A creating means which generates said 1st key from said secret key corresponding to said medium identification information read by said 1st reading means and said generation number.
The 1st decoding means that decodes said 2nd key with said 1st key generated by said creating means.

[Claim 15]It is said 2nd key decoded by the 2nd reading means that reads the 3rd key coincidence-ized with said 2nd key that said recording medium is divided per two or more recordsand is recorded on said record unitand said 1st decoding meansThe information reproducing device according to claim 14 having further the 2nd decoding means that decodes said 3rd key read by said 2nd reading meansand the 3rd decoding means that decodes said data with said 3rd key decoded by said 2nd decoding means.
[Claim 16]The information reproducing device according to claim 14wherein said memory measure memorizes said secret key of one generation and generates said secret key of other generations by an operation.
[Claim 17]The information reproducing device according to claim 14wherein a generation number of said 1st key corresponds to a generation of said secret key used by said creating means.
[Claim 18]An information reproduction mode of an information reproducing device which reproduces data currently recorded on a removable recording medium characterized by comprising the following.
A storage control step which controls memory to memorize at least one or more generations' secret key.
The 1st read-out step that reads a generation number of the 2nd key enciphered with the 1st keyand said 1st key that enciphered said 2nd keyand medium identification information of said recording medium from said recording medium.

A generation step which generates said 1st key from said secret key corresponding to said medium identification information read by processing of said 1st read-out stepand said generation number.
The 1st decoding step that decodes said 2nd key with said 1st key generated by processing of said generation step.

[Claim 19]Said recording medium is divided per two or more records.
With said 2nd key decoded by processing of the 2nd read-out step that reads the 3rd key coincidence-ized with said 2nd key currently recorded on said record unitand said 1st decoding step. With said 3rd key decoded by processing of the 2nd decoding step that decodes said 3rd key read by processing of said 2nd read-out stepand said 2nd decoding step. The information reproduction mode according to claim 18 by which the 3rd decoding step that decodes said data being included further.

[Claim 20]The information reproduction mode according to claim 18 memorizing said secret key of one generation and generating said secret key of other generations by an operation in processing of said storage control step.
[Claim 21]The information reproduction mode according to claim 18wherein a generation number of said 1st key corresponds to a generation of said secret key used by processing of said generation step.
[Claim 22]A storage control step which is a program for information reproducing devices which reproduces data currently recorded on a removable recording mediumand controls memory to memorize at least one or more generations' secret keyA read-out step which reads a generation number of the 2nd key enciphered with the 1st keyand said 1st key that enciphered said 2nd keyand medium identification information of said recording medium from said recording mediumWith said 1st key generated by processing of a generation step which generates said 1st key from said secret key corresponding to said medium identification information read by processing of said read-out stepand said generation numberand said generation step. A recording medium with which a program which a computer containing a decoding step which decodes said 2nd key can read is recorded.
[Claim 23]In a recording medium with which data is recorded or reproduced by the Information Storage Division device or information reproducing device. Were enciphered with the 1st key generated with a secret key from medium identification information which is a value peculiar to said recording mediumsaid medium identification informationand said Information Storage Division device. A recording medium while said 2nd key used in order to encipher said data is recordedwherein said 2nd key enciphered with said 1st

key is related with a generation number of said 1st key and is recorded.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about the Information Storage Division device and a methodan information reproducing devicea methodand a recording mediumIt is related with the Information Storage Division device which enabled it to record or reproduce the contents enciphered safely to a recording medium without using unjustly the contents which have copyright especially and a methodan information reproducing devicea methodand a recording medium.
[0002]
[Description of the Prior Art]In recent yearsthe recording device and recording medium which record information in digital one are spreading. Since it records for examplewithout degrading the data of an image or music and playsthese recording devices and recording media can copy data repeatedlymaintaining the quality. Howeverif it is made the owner of a copyright of an image or musicthe data of an image or music in which oneself has copyright is copied unjustly repeatedlymaintaining the qualityand there is a possibility of circulating in a commercial scene. For this reasonthere is a request which prevents copying unjustly the data which has copyright by the recording device and recording-medium side.
[0003]For examplein the mini disc (MD) (trademark) systemthe method called SCMS (Serial CopyManagement System) is used. This using the information transmitted with music data with a digital interface. Music data expresses whether it is which data of copy free (copy freedom)copy once allowed (one copy is possible)or the copyprohibited(s) (copy prohibition). When music data is received from a digital interfacean MD recorder detects SCMSand if this is copy prohibiteditMusic data is not recorded on a mini discbut if it is copy once allowedthis will be changed into copy prohibited and it will record with the received music dataand if it is copy freethis will be recorded with the received music data as it is.
[0004]Thusthe data which has copyright is prevented from being unjustly copied using SCMS in the mini disc system.
[0005]As another example which prevents copying unjustly the data which has copyrightthe contents scramble system in a Digital Versatile Disk (DVD) (trademark) system is raised. In this systemall the data that has the copyright on a disk is encipheredonly the licensed recording device can give an encryption keythe data enciphered by this is decodedand it is made as

[obtain / meaningful data]. And a recording device is designed follow regulation of not copying illegally of operation when licensed. Thusthe data which has copyright is prevented from being copied unjustly in the DVD system.
[0006]Howeverin the method which the mini disc system has adopted. If SCMS is copyonce allowed and the recording device according to regulation of changing this into copy prohibited and recording with the received data of operation will be manufactured unjustlythe copy by it cannot be prevented.
[0007]Although the method which the DVD system has adopted is effective to ROM (Read Only Memory) mediaits user is not effective in the RAM (Random Access Memory) media which can record data. In RAM mediaeven if an inaccurate person is a case where a code is undecipherableit is because the disk which operates by the licensed just recording device can newly be made by all copying the data on a disk to a new disk unjustly.
[0008]Thenin Japanese Patent Application No. 10-25310 which these people submitted previouslyThe information (it is hereafter described as medium identification information) for identifying each recording medium was recorded on the recording medium with other dataand the method of preventing from accessing the medium identification information of the recording medium only by the licensed apparatus was proposed. The data on a recording medium is enciphered by the secret key (master key) obtained by receiving medium identification information and a licenseand even if the apparatus which has not been licensed reads the enciphered datathe data is kept from making a meaning in the method. The operation is prescribed that it cannot do an unjust duplicate when each apparatus is licensed.
[0009]Since the apparatus which has not been licensed cannot access medium identification information and medium identification information serves as an individual value for each medium of everyEven if the apparatus which has not been licensed reproduces all the accessible information (enciphered) to a new mediumin the licensed apparatusthe information on the medium created by making it such cannot be correctly read as well as the apparatus which has not been licensed. Thusunjust reproduction is prevented from being performed.
[0010]
[Problem(s) to be Solved by the Invention]The secret key obtained by the license in a previous proposal needed to be common in the complete aircraft machine. This was conditions which need the medium recorded by one apparatus by other apparatus since it is refreshable (interoperability is secured).
[0011]For this reasonwhen the secret key which one apparatus received the attack by the aggressor and that apparatus held has been revealedIt will be the same as the secret key of all the apparatus having been revealednamelythe data recorded as well as the data recorded before the secret key was revealed after the secret key was revealed also had SUBJECT that it will be

decodedusing the revealed secret key.
[0012]The thing for which the secret key memorized by apparatus is updated periodically in order to prevent such a thingwhen it turns out that the secret key was revealed can be considered. By using the updated secret keythe data enciphered by the secret key will be decoded by the revealed secret key.
[0013]Howeveras mentioned abovewhen the secret key memorized by apparatus was updatedSUBJECT of it becoming impossible to decode the data enciphered using the old secret key occurred.
[0014]This invention is made in view of such a situationand. [whether two or more secret keys are memorized also including an old generation's keyand] Or even when the secret key memorized by apparatus by enabling it to create an old generation's secret key from a latest generation's secret key is updatedit enables it to decode the data enciphered using an old generation's secret key.
[0015]
[Means for Solving the Problem]Written this invention is characterized by a device comprising the following at Claim 1in order to encipher a memory measure which memorizes at least one or more generations' secret keymedium identification information of a recording medium and a creating means which generates the 1st key from a secret keyand data recorded on a recording medium. The 1st encoding means that enciphers the 2nd key to be used with the 1st key. The 1st recording device that records the 2nd key enciphered by the 1st encoding means on a recording medium with a generation number of the 1st key.

[0016]A storage control step which controls memory so that written this invention memorizes at least one or more generations' secret key to Claim 7In order to encipher medium identification information of a recording mediuma generation step which generates the 1st key from a secret keyand data recorded on a recording mediumit is characterized by a method comprising the following. The 1st encryption step that enciphers the 2nd key to be used with the 1st key. The 1st record control step that controls record to record the 2nd key enciphered by processing of the 1st encryption step on a recording medium with a generation number of the 1st key.

[0017]A storage control step which controls memory so that written this invention memorizes at least one or more generations' secret key to Claim 13In order to encipher medium identification information of a recording mediuma generation step which generates the 1st key from a secret keyand data recorded on a recording mediumit is characterized by a program of ** comprising the following.
An encryption step which enciphers the 2nd key to be used with the 1st key. A record control step which controls record to record the 2nd key enciphered

by processing of an encryption step on a recording medium with a generation number of the 1st key.

[0018]written this invention is characterized by it having been alike and comprising the following at Claim 14.
A memory measure which memorizes at least one or more generations' secret key.
The 1st reading means that reads a generation number of the 2nd key enciphered with the 1st keyand the 1st key that enciphered the 2nd keyand medium identification information of a recording medium from a recording medium.
A creating means which generates the 1st key from a secret key corresponding to medium identification information and a generation number which were read by the 1st reading means.
The 1st decoding means that decodes the 2nd key with the 1st key generated by creating means.

[0019]written this invention is characterized by it having been alike and comprising the following at Claim 18.
A storage control step which controls memory to memorize at least one or more generations' secret key.
The 1st read-out step that reads a generation number of the 2nd key enciphered with the 1st keyand the 1st key that enciphered the 2nd keyand medium identification information of a recording medium from a recording medium.
A generation step which generates the 1st key from a secret key corresponding to medium identification information and a generation number which were read by processing of the 1st read-out step.
The 1st decoding step that decodes the 2nd key with the 1st key generated by processing of a generation step.

[0020]It is characterized by a program of ** comprising the following at Claim 22 in written this invention.
A storage control step which controls memory to memorize at least one or more generations' secret key.
A read-out step which reads a generation number of the 2nd key enciphered with the 1st keyand the 1st key that enciphered the 2nd keyand medium identification information of a recording medium from a recording medium.
A generation step which generates the 1st key from a secret key corresponding to medium identification information and a generation number which were read by processing of a read-out step.
A decoding step which decodes the 2nd key with the 1st key generated by processing of a generation step.

[0021]Medium identification information which is a value with the recording medium peculiar to a recording medium according to claim 23While the 2nd key used in order to encipher data enciphered with the 1st key generated with a secret key from medium identification information and the Information Storage Division device is recordedthe 2nd key enciphered with the 1st key is related with a generation number of the 1st keyand is recorded.
[0022]In a program of the Information Storage Division device according to claim 1an Information Storage Division method according to claim 7and the recording medium according to claim 13At least one or more generations' secret key is memorizedthe 1st key is generated from medium identification information and a secret key of a recording mediumthe 2nd key used in order to encipher data recorded on a recording medium is enciphered with the 1st keyand the 2nd enciphered key is recorded on a recording medium with a generation number of the 1st key.
[0023]In the information reproducing device according to claim 14the information reproduction mode according to claim 18and a program of the recording medium according to claim 22The 2nd key that at least one or more generations' secret key was memorizedand was enciphered with the 1st key from a recording mediumA generation number of the 1st key that enciphered the 2nd keyand medium identification information of a recording medium are readthe 1st key is generated from a secret key corresponding to medium identification information and a generation number which were readand the 2nd key is decoded with the 1st generated key.
[0024]Medium identification information which is a value peculiar to a recording medium in the recording medium according to claim 23While the 2nd key used in order to encipher data enciphered with the 1st key generated with a secret key from medium identification information and the Information Storage Division device is recordedthe 2nd key enciphered with the 1st key is related with a generation number of the 1st keyand is recorded.
[0025]
[Embodiment of the Invention]An embodiment of the invention is described below. Drawing 1 expresses the example of composition of the optical-disk-recording playback equipment which applied this invention. The input part 1 outputs the signal corresponding to the alter operationwhen it is constituted by a buttona switchremote controlleretc. and alter operation is done by the user. For examplethe control circuit 2 constituted with a microcomputer etc. controls the whole device according to the predetermined computer program memorized.
[0026]The record reproduction circuit 3 has the encryption section 4 and the decoding part 5and by the pickup 6the decoding part 5 decodes the data played from the optical disc 7and it outputs it outside as a regenerative signal. When supply of a record signal is received from the exteriorthe encryption

section 4 enciphers thissupplies it to the pickup 6and is made to record on the optical disc 7.
[0027]The pickup 6 is irradiating the optical disc 7 with a laser beamand performs record reproduction of data. The spindle motor 9 is controlled by the servo circuit 8and rotates the optical disc 7. The servo circuit 8 rotates the optical disc 7 at the rate of predetermined by driving the spindle motor 9 (with for exampleconstant linear velocity). The servo circuit 8 controls a thread servo besides the tracking of the pickup 6and focusing again. The random number generation circuit 10 generates a predetermined random number by control of the control circuit 2.
[0028]The data which has structure as shown in drawing 2 is recorded on the optical disc 7. In read in area of the optical disc 7ID of the optical disc 7. The encryption disk key EKd which enciphered EDiscID enciphered with the M sequence numerals which were able to define beforehand (DiscID is called hereafter)and the disk key Kd related with the generation number by the IFEKUTIBU master key Kem is recorded. In the example shown in drawing 2the encryption disk key EKd of the generation number 1 and the generation number 3 is recorded.
[0029]DiscID is a different peculiar value for identifying the optical disc 7. The disk key Kd is a peculiar value which is different every optical disc 7 for every generation number of the master key Km of the record reproduction circuit 3 while being a peculiar value. That iswhenever the generation of the master key Km is updatedthe disk key Kdj (j= 123 --) corresponding to each generation exists (although j of Kdj shows a generation numberwhen it is not necessary to distinguish in particularit describes it also as Kd here).
[0030]M sequence numerals are predetermined cyclesand the binary of "0" and "1" is a pseudo-random binary signal (a kind of pseudo-random number) which appears at randomand DiscIDFor exampleit is enciphered by embedding in the TOC (Table Of Contents) data of a file namedirectory informationetc. based on the predetermined M sequence numerals set up beforehand. That isDiscID is recorded as a time gap of the edge of TOC data. If such encryption is performedeven if TOC data do not have M sequence numeralsit can readbut (TOC data are not enciphered) DiscID can be read if there are no M sequence numerals (it decodes). These people have proposed previously the art about the encryption based on such M sequence numerals as Tokuganhei09-288960. When these predetermined M sequence numerals receive a proper license from an owner of a copyrightthey are given to those who were licensed with the master key Km mentioned later.
[0031]The IFEKUTIBU master key Kem is calculated by combination of the master key Km and DiscID with the application of a hash function according to the formula (1) shown below.

[0032]
IFEKUTIBU master key Kem=hash (master key Km+DiscID) ... (1)
The master key Km is a secret key given only to those who were properly licensed from the owner of a copyright etc. (optical-disk-recording playback equipment) here. Herecombination of A and B means combining B behind A and considering it as 64-bit datafor examplewhen each is 32 bits.
[0033]Each sector Si (i= 12...) of the data area of the optical disc 7Comprise a header and a main data division and to a header. The encryption sector key EKsi (i= 12...) which enciphered the sector key Ksi by the disk key Kd is stored (since i of Ksi shows the number of a sector and sector keys differ for every sector hereit is described as Ksibut.). Especially when it is not necessary to distinguishit is described also as Ks.
[0034]Since two or more generations' disk key Kd (enciphered by the IFEKUTIBU master key Kem) is recorded on the optical disc 7The generation number of the used disk key Kd is also recorded on the header of each sector of a data area so that it can identify of which generation the disk key was used and enciphered. In the example shown in drawing 2since the generations of the disk key Kd currently recorded on the optical disc 7 are the generation number 1 and the generation number 3only the disk key Kd of the generation number 1 and generation number 3 is usedand the sector key EKs is enciphered.
[0035]The enciphered content data which enciphered contents data by the sector key Ksi is stored in the main data division.
[0036]Drawing 3 expresses the example of composition of the encryption section 4. The DiscID encryption decoder circuit 21 decodes the encryption disks ID and EDiscID read from the optical disc 7 based on the M sequence numerals supplied from the M sequence numerals generation circuit 22and generates DiscID. As the DiscID encryption decoder circuit 21 receives as DiscID the random number generated from the random number generation circuit 10 again and it mentioned above based on the M sequence numerals supplied from the M sequence numerals generation circuit 22It enciphers embedding at the TOC information inputtedEDiscID is generatedand it records on the optical disc 7.
[0037]The M sequence numerals generation circuit 22 can be constituted from two or more flip-flops and Exclusive-OR (IKUSUKURUSHIBUOA) circuits by which the series connection was carried outfor exampleor can also consist of a ROMan EEPROMetc.
[0038]The Km memory 24 of the Kem generating module 23 memorizes two or more master keys Km. The hash function circuit 25 of the Kem generating module 23 generates combination of the master key Km and DiscIDand computes the IFEKUTIBU master key Kem with the application of a hash function to this.
[0039]Kd encryption decoder circuit 26 decodes the encryption disk key EKd read from the optical disc 7 by the IFEKUTIBU master key Kemand generates the

disk key Kd. Kd encryption decoder circuit 26 receives again the random number generated from the random number generation circuit 10 as the disk key Kdit enciphers by the IFEKUTIBU master key Kemand it generates the encryption disk key EKdand records it on the optical disc 7.
[0040]The Ks enciphering circuit 27 receives the random number generated from the random number generation circuit 10 as the sector key Ksit enciphers by the disk key Kdand it generates the encryption sector key EKsand records it on the optical disc 7. The contents data encryption circuit 28 is the sector key Ksenciphers contents data and records it on the optical disc 7.
[0041]Although the Ks enciphering circuit 27 and the contents data encryption circuit 28 were indicated as respectively separate composition as an enciphering circuitof coursethese may consist of examples of drawing 3 as one enciphering circuit (a decoder circuit is also the same).
[0042]Nextthe example of composition of the decoding part 5 is shown in drawing 4. The EDiscID decoder circuit 41 decodes EDiscID read from the optical disc 7 based on the M sequence numerals supplied from the M sequence numerals generation circuit 42and generates DiscID. The M sequence numerals generation circuit 42 has the same composition as the M sequence numerals generation circuit 22and is made as [generate / the same M sequence numerals as the M sequence numerals generation circuit 22].
[0043]The Km memory 44 of the Kem generating module 43 memorizes two or more master keys Km. The hash function circuit 45 of the Kem generating module 43 generates combination of the master key Km and DiscIDand calculates the IFEKUTIBU master key Kem with the application of a hash function to this. This Kem generating module 43 is considered as the same composition as the Kem generating module 23and it may be made to make both serve a double purpose. Herethe master key memorized by the Km memory 24 and the Km memory 44 is explained with reference to drawing 5.
[0044]Two or more master keys Km are memorized by the Km memories 24 and 44 at order with a young generation. Drawing 5 shows the example the master key Km of the generation numbers 1 thru/or 3 is remembered to be. A generation's new master key Km is distributed via the optical disc 7 in which the new generation's master key Km was recordedfor exampleor is distributed via networkssuch as the Internet. An encryption key peculiar to the device is made to hold to each device (optical-disk-recording playback equipment) of every [which memorizes the master key Km]and after enciphering with the encryption keyit may be made to make the master key Km memorized in the Km memories 24 and 44 memorize.
[0045]The EKd decoder circuit 46 computes the disk key Kd by decoding the encryption disk key EKd read from the optical disc 7 by the IFEKUTIBU master key Kem. It computes the sector key Ks by the EKs decoder circuit 47 reading

the encryption sector key EKs currently recorded on the header of each sector Si from the optical disc 7and decoding it by the disk key Kd. The contents data decryption circuit 48 decodes the contents data which was read from the optical disc 7 and which is enciphered by the sector key Ks.
[0046]The generation discrimination circuit 49 reads the header of a data areajudges using which generation's sector key Ks the contents data currently recorded on the main data division is encipheredand outputs the decision result to the Km memory 44. The Km memory 44 outputs the master key Km memorized to the hash function circuit 45 according to the data about the generation outputted from the generation discrimination circuit 49.
[0047]Nextthe procedure in the encryption section 4 in case contents data is recorded on the optical disc 7 is explained with reference to the flow chart of drawing 6. In Step S1the DiscID encryption decoder circuit 21Judging whether EDiscID is written in read in area of the optical disc 7Kd encryption decoder circuit 26 judges whether the encryption disk key EKd is written in read in area of the optical disc 7. When judged with neither EDiscID nor the encryption disk key EKd being written init progresses to Step S2and the random number generation circuit 10 generates a 128-bit random numberand outputs it to the DiscID encryption decoder circuit 21 as DiscID.
[0048]In Step S3the DiscID encryption decoder circuit 21As supplied DiscID was mentioned above based on the M sequence numerals supplied from the M sequence numerals generation circuit 22 from the random number generation circuit 10it enciphersas it embeds into TOC informationand EDiscID is generatedand it records on read in area of the optical disc 7. The M sequence numerals which the M sequence encoder 22 supplies are given when receiving a proper license from an owner of a copyright.
[0049]Nextin step S4the hash function circuit 25 of the Kem generating module 23 reads a latest generation's master key Km from the Km memory 24 of the Kem generating module 23. The hash function circuit 25 of the Kem generating module 23At Step S5the IFEKUTIBU master key Kem is calculated by applying a hash function to combination of the master key Km read from DiscID and the Km memory 24 of the optical disc 7 according to the formula (1) mentioned aboveand Kd encryption decoder circuit 26 is supplied.
[0050]Nextin Step S6the random number generation circuit 10 generates a 40-bit random numberand outputs it to Kd encryption decoder circuit 26 as the disk key Kd. Kd encryption decoder circuit 26 enciphers the disk key Kd supplied from the random number generation circuit 10 in Step S7 by the IFEKUTIBU master key Kem received from the hash function circuit 25The encryption disk key EKd is generated and it records on read in area of the optical disc 7.
[0051]When it is judged with EDiscID and the encryption disk key EKd being written in the optical disc 7 at Step S1 on the other handProgressing to Step

S8the DiscID encryption decoder circuit 21 decodes EDiscID read from this optical disc 7 with the M sequence numerals supplied from the M sequence numerals generation circuit 22and obtains DiscID.
[0052]In step S9the hash function circuit 25 of the Kem generating module 23 reads a latest generation's master key Km from the Km memory 24 of the Kem generating module 23. The hash function circuit 25 of the Kem generating module 23 is Step S10calculates the IFEKUTIBU master key Kem according to the formula (1) mentioned above by applying a hash function to DiscID of the optical disc 7and combination of the master key Kmand supplies it to Kd encryption decoder circuit 26.
[0053]Nextin Step S11Kd encryption decoder circuit 26 decodes the encryption disk key EKd read from the optical disc 7 by the IFEKUTIBU master key Kem received from the hash function circuit 25and obtains the disk key Kd. Kd encryption decoder circuit 26 outputs the disk key Kd to the Ks enciphering circuit 27.
[0054]After Step S7 or processing of S11in Step S12the random number generation circuit 10 generates a 40-bit random numberand outputs it to the Ks enciphering circuit 27 and the contents data encryption circuit 28 as the sector key Ks. In Step S13the Ks enciphering circuit 27 Kd encryption decoder circuit 26 (when the encryption disk key EKd is recorded on the optical disc 7)Or by the disk key Kd received from the random number generation circuit 10 (when the encryption disk key EKd is not recorded on the optical disc 7)the sector key Ks received from the random number generation circuit 10 is encipheredand the encryption sector key EKs is generated. The Ks enciphering circuit 27 records the encryption sector key EKs on the header of the data area of the optical disc 7 again.
[0055]Nextin Step S14by the sector key Ksthe contents data encryption circuit 28 enciphers contents dataand records it on the main data division of the data area of the optical disc 7.
[0056]In Step S15it is judged whether each circuit of the encryption section 4 recorded all the contents data. When judged with no contents data being recorded yetit progresses to Step S16and each circuit of the encryption section 4 accesses the sector of the optical disc 7 which has not recorded data yetreturns to Step S12and repeats the same processing as the following. On the other handwhen judged with all the contents data having been recorded at Step S15each circuit of the encryption section 4 ends all the recording processings.
[0057]When receiving a proper license from an owner of a copyright as mentioned abovethe enciphered information is recorded on a recording medium by decoding enciphered DiscID and obtaining DiscID by the given predetermined M sequence mark. Even if those who have not been properly licensed from an owner

of a copyright therebyfor example reproduce the contents data of this disk to the existing recording medium (recording medium with which DiscID is not recorded)they cannot play that contents data as meaningful information.
[0058]Nextwith reference to the flow chart of drawing 7the regeneration of contents data performed by the decoding part 5 is explained. In Step S21the EDiscID decoder circuit 41 receives EDiscID which was read from read in area of the optical disc 7 and which is enciphered DiscID. The generation discrimination circuit 49 receives the header of the data area of the optical disc 7.
[0059]In Step S22after the EDiscID decoder circuit 41 decodes EDiscID and obtains DiscID based on the M sequence numerals supplied from the M sequence numerals generation circuit 42it is outputted to the hash function circuit 45 of the Kem generating module 43.
[0060]Nextin Step S23 the hash function circuit 45 of the Kem generating module 43While receiving DiscID outputted from the EDiscID decoder circuit 41According to the generation whom the generation discrimination circuit 49 distinguishedthe master key Km read from the Km memory 44 is receivedAccording to the formula (1) mentioned abovewith the application of a hash functionthe IFEKUTIBU master key Kem is computed to DiscID of the optical disc 7and combination of the master key Kmand the EKd decoder circuit 46 is supplied.
[0061]In Step S24the EKd decoder circuit 46 receives the encryption disk key EKd read from read in area of the optical disc 7. The EKd decoder circuit 46 is Step S25computes the disk key Kd by decoding this read encryption disk key EKd by the IFEKUTIBU master key Kem received from the hash function circuit 45and outputs it to the EKs decoder circuit 47.
[0062]Nextin Step S26the EKs decoder circuit 47 receives the encryption sector key EKsi of each sector read from the data area of the optical disc 7 (i= 12...). The EKs decoder circuit 47 is Step S27computes the sector key Ksi by decoding it by the disk key Kd which received this read encryption sector key EKsi from the EKd decoder circuit 46and outputs it to the contents data decryption circuit 48.
[0063]In Step S28the contents data decryption circuit 48 receives the contents data which was read from the optical disc 7 and which is enciphered. The contents data decryption circuit 48 is Step S29is decoded by the sector key Ksi which received this read contents data that is enciphered from the EKs decoder circuit 47and is outputted as a regenerative signal.
[0064]Nextin Step S30each circuit of the decoding part 5 judges whether all the contents data was read from the data area of the optical disc 7. When judged with no contents data being read yetit progresses to Step S31and each circuit of the decoding part 5 receives supply of the data of the following sector in which the optical disc 7 has not been read yetand repeats the

processing after Step S26. When judged with all the contents data having been readeach circuit of the decoding part 5 ends all the regeneration.
[0065]ThusID of a recording medium is generatedit enciphers with predetermined M sequence numeralsand only those who were properly licensed from the owner of a copyright can access the recording medium by recording on a recording medium. The data enciphered by the old generation's master key MK can also be decoded by memorizing two or more master keys Km (reproduction).
[0066]Although the Km memories 24 and 44 memorized the master key Km for every generationit may be made to generate the past generation's master key Km from a latest generation's master key Km in the embodiment mentioned above. That isthe master key Km in front of one of them is created by storing unidirectional function f in each deviceand substituting a latest generation's master key Km for the unidirectional function f. When the still older master key Km is requiredit creates one generation of the former generation's master keys Km at a time from substituting the master key Km for unidirectional function f repeatedly one by one.
[0067]As this unidirectional function fit is possible touse a Hash function and MD5 (Message Diget5) for example.
[0068]This invention can be applied also when recording or playing data to recording media other than an optical disc.
[0069]Although a series of processings mentioned above can also be performed by hardwarethey can also be performed with software. The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings with softwareOr it is installed in the personal computer etc. which can perform various kinds of functionsfor exampleare general-purposeetc. from a recording medium by installing various kinds of programs.
[0070]. Apart from a computerthis recording medium is distributed in order to provide a user with a program. The magnetic disk with which the program is recorded (a floppy disk is included)an optical disc (CD-ROM (Compact Disk-Read Only Memory).) . DVD (Digital Versatile Disk) is included. It is not only constituted by the package media which consist of a magneto-optical disc (MD (Mini-Disk) is included) or semiconductor memorybutIt comprises a ROM with which a user is provided in the state where it was beforehand included in the computer and on which the program is recordeda hard disketc.
[0071]
[Effect of the Invention]According to the program of the Information Storage Division device given in this invention and a methodan information reproducing devicea methodand a recording mediumand the recording medium. Memorize a predetermined generation's secret key and the secret key corresponding to the generation of the secret key which enciphered the data currently recorded on

the recording medium is generatedSince the data which is enciphered by the recording medium and recorded on it was decoded using the generated secret keyeven when the secret key currently recorded is updatedit becomes possible to decode the data enciphered by the old secret key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the 1 embodiment of the optical-disk-recording playback equipment which applied this invention.
[Drawing 2]It is a figure explaining the data recorded on an optical disc.
[Drawing 3]It is a figure showing the composition inside the encryption section 4 of drawing 1.
[Drawing 4]It is a figure showing the composition inside the decoding part 5 of drawing 1.
[Drawing 5]It is a figure explaining the data memorized by Km memory.
[Drawing 6]It is a flow chart explaining operation of the encryption section 4 of drawing 1.
[Drawing 7]It is a flow chart explaining operation of the decoding part 5 of drawing 1.
[Description of Notations]
1 An input part and 2 A control circuit and 3 A record reproduction circuit and 4. An encryption section and 5 A decoding part and 6 A pickup and 7. An optical disc8 servo circuitsand 9 A spindle motor and 10. A random number generation circuit21 DiscID encryption decoder circuitand 22. An M sequence numerals generation circuit23 Kem generating moduleand 24. Km memory25 hash function circuitsand 26. Kd encryption decoder circuit27 Ks enciphering circuitand 28. A contents data encryption circuit41 EDiscID decoder circuit42 M sequence numerals generation circuit43 Kem generating module44 Km memory45 hash function circuits46 EKd decoder circuit47 EKs decoder circuitand 48. A contents data decryption circuit and 49 Generation discrimination circuit